REMARKS

Claims 1-31 are currently pending in the subject application and are presently under consideration. Claims 1, 17, 20, 24, 25, and 28 have been amended as shown on pp. 2 and 4-7 of the Reply. In addition, claims 8, 30, and 31 have on p. 3 and 7 have been cancelled.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-5 and 8-16 Under 35 U.S.C §112

Claims 1-5 and 8-16 stand rejected under 35 U.S.C §112, first paragraph, as failing to comply with the enablement requirement. This rejection should be withdrawn for at least the following reasons. The Examiner has failed to establish a *prima facie* case for nonenablement.

> The standard for determining whether the specification meets the enablement requirement was cast in the Supreme Court decision of *Mineral Separation v. Hyde*, 242 U.S. 261, 270 (1916), which postured the question: is the experimentation needed to practice the invention undue or unreasonable? That standard is still the one to be applied. *In re Wands*, 858 F.2d 731, 737, 8 USPQ2d 1400, 1404 (Fed. Cir. 1988). Accordingly, even though the statute does not use the term "undue experimentation," it has been interpreted to require that the claimed invention be enabled so that ***any person skilled in the art can make and use the invention without undue experimentation***. *In re Wands*, 858 F.2d at 737, 8 USPQ2d at 1404 (Fed. Cir. 1988). ***A patent need not teach, and preferably omits, what is well known in the art***. *In re Buchner*, 929 F.2d 660, 661, 18 USPQ2d 1331, 1332 (Fed. Cir. 1991). (*See* MPEP §2164.01) (emphasis added).

Independent claim 1, as amended, recites an automation security system, comprising a plurality of automation assets; a plurality of remote devices or networks that utilize a factory protocol to transport data among end points of a communication channel; and between the plurality of automation assets and the plurality of remote devices or networks, the factory protocol utilizes at least one security field associated with the factory protocol to authenticate at least one of a requestor of the data and a supplier of the data, the security field provides at least one of a security parameter or a performance parameter, the ***factory protocol lowers encryption protocol standards for real time performance is dynamically changed or adjusted based upon***

considerations of desired security levels and real time communications and employs lightweight or heavyweight encryption mechanisms based on the performance parameter. In the subject Office Action, it is contended that applicants previously amended Claim 1, which stated "the factory protocol lowers encryption protocol standards for real time performance," was not supported within the specification. It is respectfully argued that claim 1, as it is amended, is supported by the specification. Specifically, the claimed subject matter can provide for dynamic protocol changes or adjustments based upon considerations of desired security levels and real time communications performance. Thus, if very high-end security is determined or utilized, then the amount of time to communicate data can be increased, whereas if lighter-weight protocols are employed, real time communications performance can be increased. (*See* Pg. 9, lns. 14-18; Pg. 10, lns. 19-21; Pg. 20, lns. 20-21). Thus, the claimed aspects recited in claim 1 (and associated dependent claims) have been disclosed such that a person of ordinary skill in the art can make and use the invention without undue experimentation. This rejection should be withdrawn.

II. Rejection of Claims 1-5, 8-16 and 24-27 Under 35 U.S.C. §101

Claims 1-5, 8-16 and 24-27 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Specifically, claims 1, 24 and 25 stand rejected under 35 U.S.C. § 101 because it is contended that the claims are directed to a system comprising software per se and software per se is not one of the four categories of invention. Therefore, independent claim 1 has been amended to indicate a plurality of automation assets and a plurality of remote devices or networks that utilize a factory protocol. Further, independent claims 24 and 25 have also been similarly amended to indicate an automation device that utilizes a factory protocol adapted for network communications. Therefore, withdrawal of the rejection of claims 1-5, 8-16, and 24-27 (and associated dependent claims) under 35 U.S.C. §101 is respectfully requested.

III. Rejection of Claims 1-5 and 8-24 Under 35 U.S.C. §103(a)

Claims 1-5 and 8-24 stand rejected under 35 U.S.C. §103(a) for allegedly being unpatentable over U.S. application 2002/0163920 A1 filed by Walker *et al.* (hereinafter referenced as "Walker") in view of U.S. patent 5,604,914, invented by Akiyoshi Kabe (hereinafter referenced as "Kabe"), and in further view of U.S. Patent 6,842,850 B1, invented by Dennis k. Bradstad *et al.* (hereinafter referenced as "Bradstad"). Withdrawal of this rejection is respectfully requested for at least the following reasons. Walker, in view of Kabe, further in view of Bradstad, each alone or in combination, does not disclose all aspects of the independent claims.

> [T]he prior art reference (or references when combined) must teach or suggest all claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants' claimed system and methods relate to industrial control systems, and more particularly to a system and methodology to facilitate electronic and network security in an industrial automation system. To this end, amended independent claim 1 (and similarly amended independent claims 17 and 20) recites an automation security system, comprising a plurality of automation assets; a plurality of remote devices or networks that utilize a factory protocol to transport data between the plurality of automation assets and the plurality of remote devices or networks, the factory protocol utilizes at least one security field to authenticate at least one of a requestor of the data and a supplier of the data, the security field provides at least one of a security parameter or a performance parameter, ***the factory protocol is dynamically changed or adjusted based upon considerations of desired security levels and real time communications performance and employs lightweight or heavyweight encryption mechanisms based on the performance parameter***. Neither Walker, Kabe, nor Branstad *et al.*, each alone or in any combination, teaches this novel aspect.

Walker relates to communications, and more particularly, to a method and apparatus for providing flexibility and efficiency in managing network security. However, Walker fails to disclose, teach or suggest a factory protocol that ***is dynamically changed or adjusted based upon***

considerations of desired security levels and real time communications performance and employs lightweight or heavyweight encryption mechanisms based on the performance parameter as recited in the subject claims. Kabe is similarly deficient, as noted by Examiner (*See* Office action dated January 9, 2008, page 6), who offers Branstad to remedy this deficiency. Brandstad discloses a network authentication system designed to adaptively adjust its authentication strength and speed to meet current needs based on considerations such as security policy, observed authentication error rates, alarms from host or network defenses, and processor loading (Col. 4, lns. 2-7). However, Branstad fails to disclose, teach or suggest a factory protocol that ***employs lightweight or heavyweight encryption mechanisms based on the performance parameter*** as disclosed in the claimed subject matter. Further, although Branstad disclaims a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data (Col. 1, lns. 62-64), it does not disclose plurality of remote devices or networks that utilize a factory protocol wherein the factory protocol ***is dynamically changed or adjusted based upon considerations of desired security levels and real time communications performance.***

Amended independent claim 24 recites an automation security system, comprising means for encoding a security component within a factory protocol, the factory protocol includes at least one of a security parameter or a performance parameter ***that is determined by at least one automation asset; means for transmitting the security component and the factory protocol across a network using a first standard of security if the at least one of a security parameter or a performance parameter dictates real-time performance is required, and a second standard of security if the at least one of a security parameter or a performance parameter dictates that real-time performance is not required, the first standard of security is lower than the second***; and means for the at least one automation asset to decode the security component in order to facilitate a secure communications channel across the network.

Walker discloses a method and apparatus for providing network security that implements security association to transport data among end points of a communication channel where the security association is used to authenticate the requestor and/or sender of that data (Page 4, Para. 35). Kabe discloses a communication device used to communicate among different automated factory devices that are joined through a local network (Col. 1, lns. 14-24). However, neither Walker nor Kabe disclose, teach or suggest a ***means for transmitting the security component***

and the factory protocol across a network using a first standard of security if the at least one of a security parameter or a performance parameter dictates real-time performance is required, and a second standard of security if the at least one of a security parameter or a performance parameter dictates that real-time performance is not required, the first standard of security is lower than the second. Branstad discloses an authentication system that includes a controller that dynamically selects one of a plurality of authentication mechanisms to be used in providing authentication for an exchange of message data. (Col. 1, lns. 62-64). However Branstad fails to disclose, teach or suggest utilizing a security parameter or a performance parameter ***that is determined by at least one automation asset.***

In view of the foregoing, it is readily apparent that Walker, Kabe, and Branstad, alone or in combination, fail to disclose, teach or suggest each aspect of the subject claims. Accordingly, it is respectfully requested that the rejection be withdrawn.

IV. Rejection of Claims 25-31 Under 35 U.S.C. §103(a)

Claims 25-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Walker in view of Kabe in view of Bradstad, and further in view of "Al Techniques Applied to High Performance Computing Intrusion Detection" by Susan M. Bridges *et al.* (hereinafter referenced to as "Bridges"). Similar to Walker, Kabe, and Branstad, Bridges is deficient with respect to the subject matter of amended independent claim 25, and associated dependent claims 26 and 27. Accordingly, the rejection should be withdrawn for at least the same reasons given above.

Amended independent claim 28 recites a security violation detection methodology, comprising: adapting an industrial network protocol in accordance with an intrusion detection technology; and monitoring the industrial network protocol for an attack via the intrusion detection technology, the monitoring is conducted at a first security level if real-time performance is requested and a second security level if real-time performance is not requested, the first security level is lower than the second; ***automatically performing a security action after detecting the attack, the security action includes at least one of enabling an alarm, denying network access or removing a virus.*** Walker, Kabe and Bridges are all silent in regards to ***automatically performing a security action after detecting the attack, the security action includes at least one of enabling an alarm, denying network access or removing a virus.*** Branstad discloses an authentication system that is designed to adaptively adjust its

authentication strength and speed to meet current needs based on considerations such as security policy, observed authentication error rates, alarms from host or network defenses, and processor loading (Col. 4, lns. 2-7) and provide information such as security and resource policy and alarms from host or network defenses (Col. 4, lns 34-36); however, Branstad fails to disclose, teach or suggest performing security actions of ***denying network access or removing a virus*** if a network attack is detected.

In view of the foregoing, it is readily apparent that Walker, Kabe, Branstad, and Bridges alone or in combination, fail to disclose each aspect of the subject claims. Accordingly, it is respectfully requested that the rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USB].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731